MEDICAL DEVICE CYBERSECURITY

Regional Incident Preparedness and Response Playbook Quick Start Companion Guide

November 2022

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

This Playbook was prepared by The MITRE Corporation under contract with the U.S. Food and Drug Administration. The views, opinions, and findings contained in this playbook do not constitute agency guidance, policy, or recommendations or legally enforceable requirements. Following the recommendations in this Playbook does not constitute compliance with any requirements of the Federal Food, Drug, and Cosmetic Act, or any other applicable law.

Introduction

The "*Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook*" provides a stakeholder-derived, open source, and customizable framework that HDOs may choose to leverage as a part of their emergency response plans to ultimately limit disruptions in continuity of clinical care as well as the potential for direct patient harm stemming from medical device cyber security incidents. This quick start companion guide was developed to orient new playbook users and help all users quickly identify the key parts of the playbook to turn to during an incident.

The quick start companion guide consists of tables that align with the playbook's structure: the first two tables focus on regional preparedness and response and the tables that follow focus on HDO medical device cyber incident preparedness and response. Each table distills the high-level tasks presented in the corresponding section of the playbook. The user can quickly scan the tables to identify the most appropriate section, read the guide's summary, and turn to the corresponding playbook section for more detailed information.

For example, if an HDO has evaluated their local incident response plan, but determines they are missing local and regional partnerships, they might want to start with the first task under "Regional Preparedness" (Section 5.1) in the quick start guide:

Regional Preparedness (Section 5.1)
Develop mutual aid agreements with regional partners for medical device cybersecurity, or supplements as part of broader incident response mutual aid agreements—to include loaner devices, diverting patients to a facility with operational devices, and incident response assistance https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Establish and Operationalize a Health Care Coalition – Page 10, Develop a Health Care Coalition Response Plan – Page 27) https://emsa.ca.gov/wp-content/uploads/sites/71/2017/09/HICS_Guidebook_2014_11.pdf (Coordination with External Partners – Page 19) https://www.fema.gov/sites/default/files/2020-07/fema_nims_mutual_aid_guideline_20171105.pdf (National Incident Management System Guideline for Mutual Aid)

The table header indicates the section in the playbook to turn to for more information (i.e., Section 5.1), briefly describes the activity, and may include links found in the playbook (along with specific sections and/or page numbers).

Some table headers include questions to help the HDO identify key considerations during an incident. These questions come from lessons learned during our stakeholder engagement while developing the playbook. For example, the section "Emergency Operations Plan Medical Device Cybersecurity Supplement (Section 6.1.5)" includes the following question:

- If you need to implement alternate care procedures, do you have the materials needed to implement them?

This question came from an HDO whose response plan called for falling back to paper charting if the EHR was not available but did not include ensuring that there was enough paper for staff to use during an extended downtime. In addition to having sufficient paper, HDO's must include in their plans a process for storing paper records, updating the EHR when it is back online, and properly disposing of the paper charts.

This quick start guide companion guide does not cover everything in the playbook but helps orient users to the most important preparedness and response activities.

MEDICAL DEVICE CYBERSECURITY REGIONAL INCIDENT PREPAREDNESS AND RESPONSE PLAYBOOK QUICK START COMPANION GUIDE

Regional Medical Device Cyber Incident Preparedness and Response (Section 5)

Regional Preparedness (Section 5.1)
Develop mutual aid agreements with regional partners for medical device cybersecurity, or supplements as part of broader incident response mutual aid agreements—to include loaner devices, diverting patients to a facility with operational devices, and incident response assistance. https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Establish and Operationalize a Health Care Coalition – Page 10, Develop a Health Care Coalition Response Plan – Page 27) https://emsa.ca.gov/wp-content/uploads/sites/71/2017/09/HICS_Guidebook_2014_11.pdf (Coordination with External Partners – Page 19) https://www.fema.gov/sites/default/files/2020-07/fema_nims_mutual_aid_guideline_20171105.pdf (National Incident Management System Guideline for Mutual Aid)
Establish and exchange point of contact (POC) names and contact information with regional partners, to include public key infrastructures (PKIs) for more sensitive communications, as applicable. https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Develop a Health Care Coalition Preparedness Plan – Page 17)
Ensure that all key HDO medical device cybersecurity personnel have access to alerts disseminated via the regional health emergency response communication system, such as the state Health Alert Network (HAN). https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Utilize Information Sharing Procedures and Platforms– Page 28)
Conduct joint exercises with regional partners and participate in collaborative clinical simulations. https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Plan and Conduct Coordinated Exercises with Health Care Coalition Members and Other Response Organizations – Page 20)
Identify a primary and backup regional incident command/coordination center for use during incidents (e.g., state CCIC, state Emergency Response command center). https://emsa.ca.gov/wp-content/uploads/sites/71/2017/09/HICS_Guidebook_2014_11.pdf (Integration with Community Emergency Response Partners – Page 38)
Share cybersecurity advisories and alerts with regional partners. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf (Guide to Cyber Threat Information Sharing)
Share medical device cybersecurity best practices, such as policies and plans, with regional partners. https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Share Leading Practices and Lessons Learned– Page 22)
Regional Response (Section 5.2)
Develop incident notification procedures among regional partners. (e.g., aberrant device behavior, potential incident, discovered vulnerability). https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Develop a Health Care Coalition Response Plan – Page 27)

Develop ad hoc information sharing procedures with regional partners, such as confirmation of activity ("Are you seeing this?"), feedback on manufacturer responsiveness, pointers to the HPH Sector Critical Infrastructure Protection (CIP) Program sector-wide calls held by HHS/ASPR CIP. https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Utilize Information Sharing Procedures and Platforms – Page 28)
Develop formal information sharing with regional partners, such as indicators of compromise and other relevant actionable incident information (e.g., incident source, mitigation strategies, lessons learned). https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Utilize Information Sharing Procedures and Platforms– Page 28)
Identify, develop, and test alternative communications mechanism(s) in the event primary means are compromised. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-184.pdf (Recovery Communications - Page 12) https://www.phe.gov/Preparedness/planning/hpp/reports/pmi-guidance-2019-2023/Documents/2019-2023-HPP-PMI-Guidance_508.pdf (Redundant Communications Drill Performance Measures – Page 29)
Identify and develop means for activation/use of a regional command center. https://www.fema.gov/sites/default/files/documents/fema_eoc-quick-reference_guide.pdf (National Incident Management System Emergency Operations Center How-To Quick Reference Guide) https://emsa.ca.gov/wp-content/uploads/sites/71/2017/09/HICS_Guidebook_2014_11.pdf (Establishing the Hospital Command Center (HCC) – Page 75)
Develop procedures for tracking incidents across state/region. https://www.cisa.gov/cisa-gateway (CISA Gateway Information System)
Develop procedures for requesting technical assistance and execution of mutual aid agreements with regional partners (e.g., loaner devices, diverted patients, system recovery support). https://www.fema.gov/sites/default/files/2020-07/fema_nims_mutual_aid_guideline_20171105.pdf (Mobilizing Resources (Request, Dispatch, and Response – Page 13)
HDO Medical Device Cyber Incident Preparedness and Response (Section 6)
HDO Preparedness (Section 6.1)
Medical Device Procurement (Section 6.1.1)
Consider building the cost for mitigating device vulnerabilities into the device purchase and/or maintenance fees. (e.g., ensuring that spare or extra devices will be available during an incident).
During the procurement process, consider securing a commitment by the manufacturer to participate in HDO cybersecurity exercises to build the HDO-manufacturer relationship, define roles and responsibilities of each party, and better understand the coordination efforts needed during a device incident.
Request a Software Bill of Materials (SBoM) as a procurement requirement to enable the HDO to identify and address vulnerable device components. https://healthsectorcouncil.org/wp-content/uploads/2022/05/HSCC-Model-Contract-language-for-Medtech-Cybersecurity-2022.pdf (Clause #44 - Vulnerability Management – Page 37)
Set clear expectations for vulnerability management with the manufacturer during the procurement process to reduce their risk from newly discovered vulnerabilities. https://healthsectorcouncil.org/wp-content/uploads/2022/05/HSCC-Model-Contract-language-for-Medtech-Cybersecurity-2022.pdf (All clauses related to Vulnerability Management)

Arranging for a cybersecurity preparedness user account that provides service layer access during an incident.
Set clear expectations for manufacturer support (e.g., forensics, reimaging devices, loaner systems) during response and recovery to provide a more rapid response during an incident.
Request that manufacturers provide timely notification of successful incidents against their infrastructure that can impact the HDO's clinical operations. https://healthsectorcouncil.org/wp-content/uploads/2022/05/HSCC-Model-Contract-language-for-Medtech-Cybersecurity-2022.pdf (Clause ID# 33: Vulnerability Management – Page 32)
Medical Device Inventory (Section 6.1.2) ▪ What are the critical devices that each clinical department must have to operate?
Maintain a centrally managed, baseline set of information about all medical devices (E.g., Operational status, location, network information). https://www.who.int/publications/i/item/9789241501392 (Introduction to medical equipment inventory management (World Health Organization (WHO)) https://www.oit.va.gov/library/programs/ts/edp/privacy/MedicalDeviceSecurity_V1.pdf (Support Centralized Management – Page 11)
Update this information regularly (real-time and/or when there are changes) to ensure that the inventory is current when an incident arises. https://store.aami.org/s/store#/store/browse/detail/a152E000006j66qQAA (Asset discovery, cyber risk, and patch management, Page 159)
Include device information such as, device name, description, physical location, logical location (e.g., Internet protocol address, switch port and/or wireless access point connection(s), owner/manager, maintenance parameters/status) https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Asset Management (ID.AM) Page 24)
Identify if there are embedded components (e.g., SBoM), to include details such as component version, release, and patch status. https://www.fda.gov/media/119933/download (Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff - Third Party Software Components/Software Bill of Materials – Page 11) https://www.imdrf.org/sites/default/files/2022-07/Principles%20and%20Practices%20for%20Software%20Bill%20of%20Materials%20for%20Medical%20Device%20Cybersecurity_0.pdf (Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity – DRAFT)
Identify if the device interacts with and/or has dependencies on other devices/IT resources https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Anomalies and Events (DE.AE) Page 37) https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf (Healthcare System Cybersecurity: Readiness & Response Considerations - Application Dependency Map (ADM) – Page 12)
Collect and review log files that capture device operating and/or diagnostic information (e.g., to diagnose malfunctions as cyber-related or not), ideally with a capability to interpret error codes https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Protective Technology (PR.PT) Page 36)
Hazard Vulnerability Analysis (Section 6.1.3)
Develop a Hazard Vulnerability Analysis (HVA) to assess and identify potential gaps in emergency planning. https://asprtracie.hhs.gov/technical-resources/3/Hazard-Vulnerability-Risk-Assessment/0 (Multiple resources)

https://www.calhospitalprepare.org/post/updated-hva-tool-kaiser-permanente

https://emsa.ca.gov/wp-content/uploads/sites/71/2017/09/HICS_Guidebook_2014_11.pdf (Hazard Vulnerability Analysis (HVA) – Page 17)

Review anticipated cybersecurity threats and existing mitigations to identify and manage residual cybersecurity risks (e.g., accept, avoid, transfer).

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (Page 38)

https://www.ecri.org/EmailResources/Conferences/NASRM/Session%205b%20Hazard%20Vulnerability%20Assessments%201%20slide%20pp.pdf

Medical Device Cybersecurity Support to the Hospital Incident Management Team (HIMT) (Section 6.1.4)

- Does our IR plan, include a risk-based plan for bringing medical devices back online?
- Do our emergency cybersecurity plans include workarounds/contingencies for extended downtimes (e.g., days, weeks, months)?
- Have we considered what the "blast radius" (i.e., the downstream impacts of operation disruptions on your organization and to neighboring health systems) as part of preparedness efforts? (e.g., device dependencies result in non-functional devices, patient diversions)

If an incident includes medical device cybersecurity concerns, include Medical-Technical Specialists with cybersecurity and medical device expertise as part of the activated HIMT.

https://emsa.ca.gov/wp-content/uploads/sites/71/2017/09/Appendix-D-Potential-Candidates_3.pdf

Review the Healthcare and Public Health Sector Coordinating Council's (HSCC) Cybersecurity Working Group (CWG) "Operational Continuity – Cyber Incident (OCCI)" checklist to identify actions to be taken during a cyber incident by the various roles in the HIMT.

https://healthsectorcouncil.org/occi/

Identify if there are any cybersecurity decisions and/or actions that should be sanctioned (e.g., through policy) by a senior leadership champion, such as the CIO, to facilitate timely decision making during an incident.

https://emsa.ca.gov/wp-content/uploads/sites/71/2017/09/HICS_Guidebook_2014_11.pdf Hospital Incident Command System - Planning should ensure engagement of senior leadership and stakeholders – Page 15)

Determine if any IR roles require external support (e.g., manufacturer(s), maintenance contractor(s), peer HDOs, regional partners, trade associations, H-ISAC) and what that support will entail.

https://emsa.ca.gov/wp-content/uploads/sites/71/2017/09/HICS_Guidebook_2014_11.pdf Hospital Incident Command System Guidebook - Hospital Incident Management Team Overview – Page 43)

Identify any additional medical device cybersecurity HIMT roles and responsibilities. (E.g., Information Security Officer (ISO, Chief Information Officer (CIO), Specialized Technical Experts, Medical Device Cybersecurity Liaison, Other HDO Support Staff).

https://emsa.ca.gov/wp-content/uploads/sites/71/2017/09/Appendix-D-Potential-Candidates_3.pdf

Emergency Operations Plan Medical Device Cybersecurity Supplement (Section 6.1.5)

- If we need to implement alternate care procedures, do we have the materials needed to implement them?

Develop an Emergency Operations Plan (EOP) to describe how the HDO will respond to and recover from a threat, hazard, or other incident.

https://asprtracie.hhs.gov/technical-resources/84/emncy-operations-plans-emncy-management-program/1#:~:text=The%20emergency%20operations%20plan%20(EOP,by%20department%2C%20etc.)

https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Develop a Health Care Organization Emergency Operations Plan – Page 26)

https://emsa.ca.gov/wp-content/uploads/sites/71/2017/09/HICS_Guidebook_2014_11.pdf (All-Hazards Emergency Operations Plan (EOP) – Page 16)

Incident Response Communications Plan (Section 6.1.6)

- Does our communication plan leverage different communications vehicles for different stakeholders (e.g., patients, hospital staff)?

Include medical device cyber incident-specific communications in an overall HDO IR Communications Plan, specifying incident sharing expectations for all participants.

https://emsa.ca.gov/wp-content/uploads/sites/71/2017/07/IT-Failure-IPG.pdf (Preparedness - #5 Communications plan)

Include planned frequency of communications with internal and external stakeholders in an overall HDO IR Communications Plan.

Identify sources of vulnerability, threat, and other situational awareness information, as well as mechanisms to ingest, analyze and share data.

https://www.fema.gov/sites/default/files/2020-04/CPG201Final20180525.pdf (Page 13)

Develop communication templates to prepare for different IR messaging needs.

Training (Section 6.1.7)

- Are we engaging the relevant stakeholders (e.g., emergency preparedness, biomedical engineering, IT, clinicians) in exercises and planning?

Develop user awareness training to facilitate early detection of cyber incidents.

https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf (Top 10 Tips for Cybersecurity in Health Care- Establish a Security Culture – Page 1)

Create or participate in exercises designed to simulate realistic cyber incidents.

https://www.mitre.org/sites/default/files/2022-09/pr_14-3929-cyber-exercise-playbook%20.pdf

https://www.cisa.gov/sites/default/files/publications/Healthcare-and-Public-Health-Sector-Cyber-CTEP-Situation-Manual-508-20220713.docx

HDO Detection and Analysis Phase (Section 6.2)

Incident Detection and Validation (Section 6.2.1)

Identify or otherwise establish that a cyber incident has occurred.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (3.2.2 Signs of an incident- page 26; Incident Handling Checklist – Page 42)

Incident Categorization and Prioritization (Section 6.2.2)

Define classes of medical device cyber incidents to help prioritize incidents and determine the appropriate level of response.

https://portal.ct.gov/-/media/DAS/BEST/Security-Services/Incident-Response-Plan-template.doc (State of Connecticut Sample Incident Response Plan – Incident Classification - Page 14)

Establish an escalation list that ties medical device cybersecurity IR decision making responsibilities to specific roles in the HIMT hierarchy, in keeping with higher incident severity levels.

https://healthsectorcouncil.org/occi/

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (3.2.6 Incident Prioritization - page 32)

Incident Response – Reporting (Section 6.2.3)

Identify the formal and informal reporting obligations that accompany discovery of a medical device cyber incident. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (3.2.7 Incident Notification - page 33)
Incident Response – Analysis (Section 6.2.4)
Gather data to determine the full incident impact, which will inform the containment strategy. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (3.2.4 Incident Analysis - page 28)
Preserve evidence and chain of custody (i.e., recording all transfers of evidence and maintaining logs detailing the evidence and how it was handled) if the incident may involve potential criminal activity https://www.cisa.gov/sites/default/files/publications/cisa-insights_chain-of-custody-and-ci-systems_508.pdf (CISA Chain of Custody and Critical Infrastructure Systems)
Conduct a digital forensics investigation order to identify evidence of a crime, attribute evidence to suspects, or simply to investigate an intrusion to understand its nature and extent. Identify and deploy external forensics experts as necessary. https://nij.ojp.gov/digital-evidence-and-forensics (Multiple links) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf
Incident Response – Documenting (Section 6.2.5)
Record all activities undertaken during cybersecurity IR, from incident discovery to containment and post-activity. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (3.2.5 Incident Documentation - page 30)
HDO Containment, Eradication, and Recovery Phase (Section 6.3)
Execute the EOP to initiate containment, eradication, and recovery activities to minimize the impact to healthcare delivery, halt the active cybersecurity disruption, assess the damage, and restore normal business operations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (3.3.1 Choosing a Containment Strategy - page 35)
HDO Post-Activity Phase (Section 6.4)
Lessons Learned (Section 6.4.1)
Identify lessons learned to improve the existing plan and the HDO's response to future incidents. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (Lessons learned - Page 38)
Plan Updates (Section 6.4.2)
Document post-incident insights such as what worked, what didn't, and ideas for the future. https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (. Develop a Health Care Organization Emergency Operations Plan – Page 27) https://www.cisa.gov/uscert/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-IM.pdf (Conduct an after-action review of plan activities – Page 26)